



<p>Havells India Limited</p> <p>Havells India Backup and Restore Management Policy</p> <p>Version 1.1</p> <p>Internal</p>	 <p>HAVELLS</p>
---	---

Havells India

Backup and Restoration Management Policy

Version 1.1

Havells India Limited Havells India Backup and Restore Management Policy Version 1.1 Internal	
--	---

Document Control


S. No.	Type of Information	Document Data
1.	Document Title	Havells India Backup and Restoration Management Policy
2.	Document Code	HBRMP
3.	Date of Release	28th June 2022
4.	Document Superseded	1.0
5.	Document Approvers	Mr. Pramod Mundra and Mr. Ramanand Jha
6.	Document Owner	Information Security Head
7.	Documents Author(s)	Mr. Sanjay Roongta and Mr. Neeraj Nagpal

Document Approvers

S. No.	Approver	Approver Designation	Approver Contact
1.	Pramod Mundra	Chief Information Officer (CIO)	Pramod.Mundra@havells.com
2.	Ramanand Jha	Information Security Head	ramanand.jha@havells.com

Document Change Approvals

Version No	Revision Date	Nature of Change	Date Approved
1.0	NA	Initial Version	18th Feb 2022
1.1	28 th June 2022	Audit Trail retention from 90 to 180 days as per Cert-In directions	28 th June 2022

Havells India Limited Havells India Backup and Restore Management Policy Version 1.1 Internal	 HAVELLS
--	---

Document Scope

This document shall be applicable to the IT department and the employees/third parties referred henceforth shall include the staff working with IT department and/or handling, processing, and managing information/information assets of Havells.

Document Distribution

The Information Security Head shall distribute this policy to all employees working with IT department and/or handling, processing, and managing information/information assets of Havells by uploading it on the intranet/by sharing it via email/as appropriate.

Document Conventions

All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

Table of Contents

1. Purpose	5
1.1 Scope	5
1.2 Responsibility	5
1.3 Enforcement	5
1.4 Authority.....	5
2. Policy.....	6
2.1 Backup planning	6
2.2 Backup Schedule	7
2.3 Labelling of backup media.....	8
2.4 Handling and storage of on-prem backup media	8
2.5 Logs of backup	9
2.6 Retention of data	9
2.7 Restoration	9

<p>Havells India Limited</p> <p>Havells India Backup and Restore Management Policy</p> <p>Version 1.1</p> <p>Internal</p>	
---	---

1. Purpose

The purpose of the Backup and Restoration Management Policy is to ensure that the Business critical information assets of Havells are backed-up and are recoverable as and when required. This would also ensure that all backups of information assets are in accordance with the approved business and technical requirements and are planned, implemented, and tested in a controlled and consistent manner.

1.1 Scope

This policy shall be applicable to the IT department (Backup Team) and the employees/third party who deal with Havells' IT and/or handle, process or manage information/information assets of Havells.

1.2 Responsibility

It is the responsibility of the IT Backup team and respective or concerned business/functional team to implement and maintain the guidelines as defined in the Backup and Restoration Management Policy.

1.3 Enforcement

All Employees and/or third party, who deal with Havells' IT and/or handle, process or manage information/information assets of Havells, must comply with this policy. All statements in the document are mandatory requirements. Failure to observe these requirements may be construed as non-compliance to the policy.

- a) Non-compliance with this policy shall be dealt with in accordance with the approved management process.
- b) Employees and third parties who breach this policy shall be subject to disciplinary action.

Requests for deviations from this policy must be documented and managed using the approved process. Any requests for deviations from this policy must be approved in accordance with the *Security Exception Management Policy*.

1.4 Authority

The Chief Information Officer (CIO) and Information Security Head approves and enforces this policy and mandates processes to monitor and ensure compliance to this policy.

2. Policy

Backup & restoration management is the process of ensuring that the information generated during the course of conducting business is available at all times. The backup & restoration management process also ensures that in the event of a disaster, this information can be restored with minimum data loss.

In order to implement an effective backup & restoration management process, Havells needs to ensure that data pertaining to all the applications/shared drive is regularly backed up. Restoration shall also be performed on a periodic basis to ensure the integrity and availability of backed up data.

2.1 Backup planning

Business critical information shall be backed up and tested for restoration to ensure availability of such information as required. Havells shall use backup tool for taking backups. Backup Administrator should configure the backup tool as per the backup policy.

- a) The performing backup procedures for all business applications listed as below: backup administrator is responsible for
 - i. SAP applications (critical and non-critical modules)
 - ii. Non-SAP applications (critical and non-critical)
- b) The following types of backup shall be performed by the backup team for the data pertaining to all the systems/applications:
 - i. Daily backup
 - ii. Weekly backup
 - iii. Monthly backup
 - iv. Yearly backup
- c) The Backup team shall maintain backup calendar(maintained in Backup System) in adherence to backup policy and backup tracker should be maintained for any changes which should be reviewed and approved by respective Backup lead on an half yearly basis. The backup calendar shall include (but not limited to):
 - i. Information to be backed up;
 - ii. Name of the system hosting the information (e.g. server name);
 - iii. The type of backup – i.e. incremental/full etc.;
 - iv. Backup periodicity – daily, weekly, monthly, based on the criticality of information;
- d) In case the backup activity fails, the Backup Administrator should perform root cause analysis, prepare a corrective action plan, and report the issue(s) to respective team. A manual backup is recommended in this case.

2.2 Backup Schedule

The backup shall be performed on daily, weekly, and monthly basis (as applicable) as per the schedule mentioned below.

SAP Application (Critical and non-critical modules)

Backup Name	Schedule	Backup Type
Online Database Backup	Daily, Weekly, Monthly, Yearly	Full
Online Filesystem Backup(as per business requirement)	Weekly, Monthly, Yearly	Full
Transaction log Backup	Every 30 Minute	Full

Critical Non-SAP Applications


Backup Name	Schedule	Backup Type
Online Database Backup	Daily, Weekly, Monthly, Yearly	Full
Online Filesystem Backup(as per business requirement)	Weekly, Monthly, Yearly	Full
Online Differential DB Backup (as per business requirement)	Every 6 Hours	Differential
Online Log Backup (as per business requirement)	Every 30 Minutes	Full

Non-Critical Non-SAP Applications

Backup Name	Schedule	Backup Type
Online Database Backup	Daily, Weekly, Monthly, Yearly	Full
Online Filesystem Backup(as per business requirement)	Weekly, Monthly, Yearly	Full
Online Differential DB Backup (as per business requirement)	Every 6 Hours	Differential

OS Backup (VMware, and Windows)

Backup Name	Schedule	Backup Type
Online BMR Backup (Windows)	Weekly, Monthly	Full
Online Snapshot Backup (Hyper-V/ VMware VM)- Production	Weekly, Monthly	Weekly, Monthly –Full
Online Snapshot Backup (Hyper-V / VMware VM) - Dev/QA	Weekly, Monthly	Weekly, Monthly –Full

Havells India Limited Havells India Backup and Restore Management Policy Version 1.1 Internal	
--	---

Shared File storage (NAS Storage)

Backup Name	Schedule	Backup Type
NAS Storage	Daily	Incremental

Cloud Backup [AWS (Amazon Web Services)/ Microsoft Azure / GCP (Google cloud platform)]

Backup Name	Schedule	Backup Type
AWS (IaaS) Production	Daily, Weekly, Monthly, Yearly	Image Backup Full
AWS (IaaS) Dev/QA	Daily, Weekly, Monthly, Yearly	Image Backup Full
AWS (RDS)	Daily	DB Backup Full
Microsoft Azure (IaaS)	Daily, Weekly, Monthly, Yearly	Image Backup Full
Microsoft Azure (PaaS)	Daily	File System Backup Full
Microsoft Azure (DaaS) MS SQL	Daily, Weekly, Monthly, Yearly	DB Backup Full
Microsoft Azure (DaaS) MY SQL	Daily	DB Backup Full

2.3 Labelling of backup media

The backup media is barcoded/labelled manually and all the information for the data backed up into the media is stored in the backup tool. Havells' backup team shall keep a track of all the barcoded media which is sent to offsite.

2.4 Handling and storage of on-prem backup media

- a) Storing monthly tape backup
 - i. All monthly tapes of Noida Data Centre (1-year retention) shall be sent offsite (Sahibabad location / Noida Head Office location) and kept in a fire-proof cabinet;
 - ii. All monthly tapes of Bangalore Data Centre (1-year retention) shall be sent offsite (Noida Head Office location) and kept in a fire-proof cabinet;
- b) Backup Administrator shall ensure that backups are not maintained on the same physical media that contains the original data as redundancy of data might not be achieved;
- c) As per the storage of backup process, one copy of the identified back up media shall be stored at an off-site location which shall be at least 5 km from the onsite location;
- d) An appropriate backup movement register / soft copy shall be maintained, detailing the person who has accessed the backup, the destination location, media type and count of storage media devices;
- e) The key to the cabinet should be available only with the Backup Administrator in charge of the backup and with the security personnel/ IT authorized team member in case of an emergency; and

- f) Whenever the backup media is moved to and from off-site location, it should be carried in sealed and tamper-proof envelope or pouch or briefcase or properly packed cartoon and the backup movement register/Soft copy shall be updated.

2.5 Logs of backup

Havells' backup Team shall maintain details of backup jobs activities carried out in the backup tool. The Audit trail needs to be maintained for a period of 180 days

2.6 Retention of data

The retention timelines to be followed for types of backup is given below:

On- prem	
Daily backup	1 week
Weekly backup	1 month
Monthly backup	1 year
Yearly backup	10 years
Cloud	
Daily backup	1 week
Weekly backup	1 month
Monthly backup	1 year
Yearly backup	10 years
Daily backup (AWS RDS)	35 days
Daily backup (MS PaaS)	30 days
Daily backup (MS DaaS)	35 days
Yearly Backup (Cloud-Azure IaaS)	10 Years
Yearly Backup (Cloud-AWS IaaS)	10 Years

2.7 Restoration

- A restoration calendar shall be maintained to include the applications restoration drill / test schedule or a limited DR Drill for critical applications ;
- Restoration shall be performed for critical SAP modules and critical non-SAP applications half yearly / annually;
- The backup administrator should maintain the backup restoration request in ITSM tool;
- In case of an incident of system crash or database does not open, a business user/IT Team raises a backup restoration request through an email / ITSM / verbal
- The concerned department/functional head shall approve the restoration request. The department/functional head shall ensure that business user is authorized to access the data that is requested for restoration;
- Post approval of department/functional head, the request is forwarded to the Backup team; and
- It is the responsibility of the business user to review if the restoration of the requested data is complete and accurate.